_General

Created by Dennis Underwood, last modified on May 24, 2022

It is very rare, possibly never, that an attacker performs an entire attack from within one process.

The fact that an attack tool or a Windows library is using multiple processes and Windows programs is sometimes invisible to users of the malware (aka, the criminals).

Process behaviors represent an important source of variables during Cyber Crucible decision making, which involves behavioral indicators from a variety of sources.

Sometimes these process behaviors may ultimately result in a process suspension from data theft or ransomware encryption, and can be traced from attacker entry point through the system, to ultimate extortion software execution.

Other times, process tracing can identify unauthorized remote access, fraud, insider threat, or unexpected software, but not data extortion. So, not something that Cyber Crucible's data extortion prevention software will automatically suspend, but still something you want to know about.

Whether the process data is part of a data extortion attack, something else of note, or just program behavior, the programs source and destination information, to include program arguments, are made available. This provides a rich set of data to trace attackers, including ones leveraging "living off the land" tactics.

Below is a screenshot of the type of data that can be gathered from process creations.

CC_process_creation_demo.mp4

Revision #1
Created 2026-05-18 20:27:20 UTC by Dennis Underwood
Updated 2026-05-18 20:27:20 UTC by Dennis Underwood